

In the Claims

Claims pending

- At time of the Action: Claims 1-6, 8-20 and 26-38.
- After this Response: Claims 1-6, 8, 10-14, 17-20, 26-32 and 34-38.

Currently Amended Claims: Claims 1, 5, 6, 12, 26, 31 and 32.

Currently Canceled claims: Claims 9, 15, 16 and 33.

1. (Currently Amended) A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method for protecting digital media comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating one or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the one or more codes do not employ M_2 or an encryption of M_2 , and M_2 cannot be derived from these calculations of one or more codes, the generating further comprising:

~~finding a value of a variable per message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing k produces a result equivalent to M_2 , wherein g is a fixed element of order q in a fixed group, and H_0 is a~~

~~predefined hash function instantiated by using a keyed version of a secure hash function; and~~

~~when such a value of k is found, calculating two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k ; and~~

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2 , wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of k is found, calculating the two or more codes, where one code is r and another is s , with r being calculated using another predefined mathematical function employing M_1 and g^k , $r = H_1(M_1, g^k)$, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r , $s = k/(r + 1) - x H_2(M_1, g^k) \bmod q$; and

reporting the one or more codes, by which reporting the one or more codes facilitates a cryptographic technique for protecting digital media.

2. (Previously Presented) The medium as recited in claim 1, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported one or more codes.

3. **(Previously Presented)** The medium as recited in claim 1, wherein two or more codes are generated by the generating and reported by the reporting.

4. **(Previously Presented)** The medium as recited in claim 3, wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code.

5. **(Currently Amended)** The medium as recited in claim 3, wherein the message M has a ~~pre-determined~~ defined length and a length of a combination of two or more codes is less than the message's ~~pre-determined~~ defined length.

6. **(Currently Amended)** The medium as recited in claim 3, wherein M_2 has a ~~pre-determined~~ defined length and a length of a combination of two or more codes is less than or equal to the ~~pre-determined~~ defined length of M_2 .

7. **(Previously Canceled)**

8. **(Previously Presented)** The medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing k produces a result equivalent to M_2 , wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code, the calculation of at least one code employs non-linear mathematical function, and where each calculation incorporates k .

9. (Canceled)

10. (Previously Presented) The medium as recited in claim 3, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported codes.

11. (Previously Presented) A computing device comprising:
an output peripheral device;
the medium as recited in claim 1.

12. (Currently Amended) A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another, wherein the message M has a defined length and a length of a combination of two or more codes is less than the message's defined length and M_2 has a defined length and a length of a combination of two or more codes is less than or equal to the defined of M_2 ;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2 ~~or an encryption of M_2~~ , and M_2 cannot be derived from these calculations of two or more codes, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2 , wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using keyed versions of a secure hash function;

when such a value of k is found, calculating the two or more codes, where one code is r and another is s , with r being calculated using another predefined mathematical function employing M_1 and g^k , $r = H_1(M_1, g^k)$, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r , $s = k/(r + 1) - x H_2(M_1, g^k) \bmod q$; and reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

13. (Previously Presented) The medium as recited in claim 12, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported two or more codes.

14. (Previously Presented) The medium as recited in claim 12, wherein the calculation of at least one code employs a non-linear mathematical function.

15. (Canceled)

16. (Canceled)

17. (Previously Presented) The medium as recited in claim 12, wherein one calculated code is r and another is s , with r being calculated using another predefined mathematical function employing M_1 and g^k , and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r .

18. (Previously Presented) The medium as recited in claim 17, wherein the predefined mathematical function for s is non-linear.

19. (Previously Presented) The medium as recited in claim 17, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported codes r and s .

20. (Previously Presented) A computing device comprising:
an output peripheral device;
the medium as recited in claim 12.

26. (Currently Amended) A method for facilitating digital security, the method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2 ~~or an encryption of M_2~~ , and M_2 cannot be derived from these calculations of one or more codes, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2 , wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using keyed versions of a secure hash function;

when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k , wherein one calculated code is r and another calculated code is s , with r being calculated using another predefined mathematical function employing M_1 and g^k , $r = H_1(M_1, g^k)$, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r , $s = k/(r + 1) - x H_2(M_1, g^k) \bmod q$; and

reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

27. (Previously Presented) The method as recited in claim 26 further comprising producing a digital signature (*DS*) comprising M_1 and the reported two or more codes.

28. (Previously Presented) A digital signature (*DS*) produced by the method as recited in claim 27 and embodied on a computer-readable medium.

29. (Previously Presented) A digital signature (*DS*) produced by the method as recited in claim 27 and embodied as human-readable indicia on a human-readable medium.

30. (Previously Presented) The method as recited in claim 26, wherein the calculation of at least one code employs a non-linear mathematical function.

31. (Previously Presented) The method as recited in claim 26, wherein the message M has a ~~pre-determined~~ defined length and a length of a combination of two or more codes is less than the message's ~~pre-determined~~ defined length.

32. (Previously Presented) The method as recited in claim 26, wherein M_2 has a ~~pre-determined~~ defined length and a length of a combination of two or more codes is less than or equal to the ~~pre-determined~~ defined length of M_2 .

33. (Canceled)

34. (Previously Presented) The method as recited in claim 33, wherein the predefined mathematical function for s is non-linear.

35. (Previously Presented) The method as recited in claim 33, wherein the predefined mathematical function for s is quadratic.

36. (Previously Presented) The method as recited in claim 26 further comprising producing a message comprising M_1 and the reported codes.

37. (Previously Presented) A computer-readable medium embodying a message produced by the method as recited in claim 36, by which the message functions with a processor to protect digital media.

38. (Previously Presented) A method comprising:
producing a message produced by the method as recited in claim 36 as human-readable indicia on a human-readable medium.